(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
16 octobre 2003 (16.10.2003)

PCT

(10) Numéro de publication internationale
WO 03/085881 A1

(51) Classification internationale des brevets[7] : H04L 9/06

(21) Numéro de la demande internationale :
PCT/FR03/01032

(22) Date de dépôt international : 2 avril 2003 (02.04.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/04341 8 avril 2002 (08.04.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **OBERTHUR CARD SYSTEMS S.A.** [—/FR]; 102, boulevard Malesherbes, F-75017 Paris (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(pour US seulement)* : **GIRAUD, Christophe** [—/FR]; 7, Rue Fustel de Coulanges, F-75005 Paris (FR).

(74) Mandataire : **SANTARELLI**; 14, avenue de la Grande Armée, Boîte postale 237, F-75822 Paris Cedex 17 (FR).

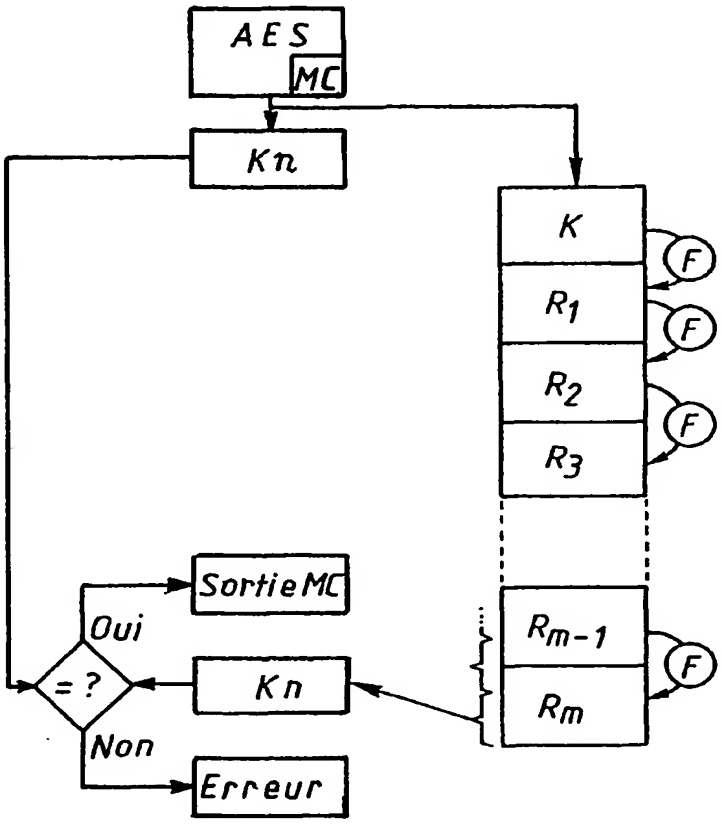
(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet

[Suite sur la page suivante]

(54) Title: METHOD FOR MAKING SECURE AN ELECTRONIC ENTITY WITH ENCRYPTED ACCESS

(54) Titre : PROCEDE DE SECURISATION D'UNE ENTITE ELECTRONIQUE A ACCES CRYPTE



(57) **Abstract:** The invention concerns a method for protecting an electronic entity with encrypted access, against DFA (Differential Fault Analysis) attacks which consists in: storing the result of a selected step (R_m, K_n) of an iterative process forming part of the cryptographic algorithm and in performing once more at least part of the steps of said iterative process up to a new computation of a result corresponding to the one which has been stored, comparing the two results and denying distribution of an encrypted message (MC) if they are different.

(57) **Abrégé :** Protection d'une entité électronique à accès crypté, contre les attaques du type DFA. On mémorise le résultat d'une étape choisie (R_m, K_n) d'un processus itératif faisant partie de l'algorithme cryptographique et on refait au moins une partie des étapes de ce processus itératif jusqu'à recalculer un résultat correspondant à celui qui a été mémorisé, on compare les deux résultats et on interdit la diffusion d'un message crypté (MC) s'ils sont différents.

WO 03/085881 A1

européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

Procédé de sécurisation d'une entité électronique à accès crypté

L'invention se rapporte à un procédé de sécurisation d'une entité électronique à accès crypté, telle que par exemple une carte à microcircuit, le perfectionnement visant plus particulièrement à détecter les attaques connues sous l'abréviation DFA (Differential Fault Analysis, en anglais). L'invention vise particulièrement à sécuriser des algorithmes connus tels que l'AES ou le DES.

Certaines entités électroniques à accès crypté, notamment les cartes à microcircuit, sont vulnérables à des attaques dites DFA consistant à perturber le déroulement de l'algorithme cryptographique de façon à changer la valeur d'un résultat intermédiaire, à traiter la différence obtenue entre le message chiffré normalement et le message chiffré avec erreur et à en déduire des informations sur la clé secrète de l'entité électronique. Les erreurs sont très faciles à produire sur une carte à microcircuit, en intervenant sur l'environnement extérieur, par exemple en provoquant un pic de tension, en soumettant la carte à un éclair lumineux (notamment à l'aide d'un faisceau laser), en faisant varier brutalement la fréquence de l'horloge extérieure, etc...

Parmi les algorithmes les plus utilisés, on peut citer le DES (Data Encryption Standard, en anglais) et surtout l'AES (Advanced Encryption Standard, en anglais). On rappelle que les deux algorithmes AES et DES ont en commun d'appliquer à un message d'entrée une succession de groupes d'opérations dits "rounds" sous le contrôle d'une série de sous-clés respectives, successivement élaborées à partir d'une clé initiale secrète, spécifique de l'entité électronique considérée. C'est cette clé initiale (notée K ci-après) que le fraudeur tente de reconstituer. Une partie de l'algorithme est consacrée à l'élaboration des sous-clés en mettant en œuvre un processus d'extension de clé par une fonction F, non linéaire dans le cas de l'AES. La fonction est appliquée à ladite clé initiale, puis à nouveau au résultat de l'application de ladite fonction et ainsi de suite. Les sous-clés sont élaborées à partir de cette succession de résultats intermédiaires issus de la clé initiale K.

Jusqu'à présent, les attaques de type DFA sont considérées comme inexploitables en pratique vis-à-vis de l'algorithme de type AES. Cependant, des études à l'origine de l'invention ont permis de mettre en évidence qu'une triple

attaque du type DFA, en synchronisme avec certaines applications de la fonction F et le début du dernier "round", permet de retrouver tous les octets de la dernière sous-clé dans le cas où ladite clé d'entrée K est codée sur 128 bits, ce qui est actuellement le cas pour la plupart des systèmes où l'algorithme AES est utilisé. La connaissance de ces informations permet de retrouver la clé d'entrée.

L'invention offre une parade simple et efficace à ce type d'attaque. L'invention concerne un procédé de sécurisation d'une entité électronique à accès crypté, laquelle comprend des moyens d'exécution d'un algorithme cryptographique consistant à appliquer à un message d'entrée une succession de groupes d'opérations dits "rounds" faisant intervenir une série de sous-clés respectives, successivement élaborées par un processus itératif mis en œuvre à partir d'une clé initiale, caractérisé en ce qu'il consiste à mémoriser le résultat d'une étape dudit processus itératif, à refaire au moins une partie des étapes dudit processus itératif jusqu'au recalcul d'un résultat correspondant à celui qui a été mémorisé, à comparer la valeur dudit résultat mémorisé à la valeur du résultat recalculé correspondant et à interdire la diffusion d'un message crypté résultant de la mise en œuvre dudit algorithme si ces deux valeurs sont différentes.

En effet, si une erreur, due à une attaque DFA, intervient pendant le processus itératif d'élaboration des sous-clés, alors le résultat mémorisé et le résultat recalculé correspondant sont forcément différents car il est impossible de reproduire deux fois de suite la même "erreur" dans la pratique.

Par exemple, un résultat mémorisé, dit résultat intermédiaire, peut être l'une des étapes du processus dit de diversification de clé consistant à appliquer une fonction F non linéaire au résultat de l'étape analogue précédente. On peut aussi mémoriser l'une des sous-clés et recalculer cette sous-clé à partir d'une étape antérieure dudit processus itératif. Par exemple, on mémorise la dernière sous-clé.

L'invention sera mieux comprise et d'autres avantages de celle-ci apparaîtront plus clairement à la lumière de la description qui va suivre, donnée uniquement à titre d'exemple et faite en référence aux dessins annexés dans lesquels :

- la figure 1 est un schéma d'une entité électronique telle qu'une carte à microcircuit, susceptible de mettre en œuvre le procédé de l'invention ;

- la figure 2 est un organigramme illustrant l'algorithme dit AES ;

- la figure 3 est un organigramme illustrant la mise en œuvre de l'invention à titre de complément dans l'exécution de l'AES ; et

- la figure 4 est un organigramme illustrant l'algorithme DES auquel l'invention peut aussi s'appliquer.

Sur la figure 1, on a représenté une entité électronique 11, formant ici une carte à microcircuit avec ses composants essentiels, à savoir un ensemble de plages de contact 12, métalliques, permettant de connecter le microcircuit 13 contenu dans la carte à un lecteur de carte, serveur ou analogue avec lequel ladite carte à microcircuit va pouvoir échanger des informations après une phase d'authentification mettant en œuvre un algorithme connu à clé secrète, par exemple l'algorithme AES ou l'algorithme DES. Classiquement, le microcircuit 13 se décompose en un microprocesseur 14, dont certains accès sont connectés aux plages de contact, et une mémoire M couplée au microprocesseur. Lorsque la carte est couplée à une unité extérieure pour remplir une fonction donnée (transaction financière, accès à un service téléphonique ou télématique, contrôle d'accès, etc...), une phase d'authentification est mise en œuvre dans la carte. Ce processus est programmé dans le microcircuit 13 et une partie de la mémoire M lui est dédiée.

Par exemple, la phase d'authentification met en œuvre un algorithme AES dont le fonctionnement va être rappelé en référence à la figure 2. L'algorithme AES s'opère à partir d'un message d'entrée ME transmis en clair par l'unité extérieure à laquelle l'entité électronique se trouve couplée. L'entité 11 possède aussi une clé secrète K, mémorisée, et l'algorithme consiste à transformer le message ME jusqu'à obtenir un message chiffré MC à la suite d'un certain nombre de transformations opérées avec intervention d'un certain nombre de sous-clés K_0, K_1, K_2, ..., K_{n-1}, K_n. D'autre part, une fonction non linéaire F est programmée dans l'entité électronique pour s'appliquer successivement, d'abord à la clé K, puis au résultat R_1 la transformation de la clé K par la fonction F, puis au résultat R_2 de la transformation du résultat R_1 par la même fonction F et ainsi de suite. Les différentes sous-clés K_0 ... K_n sont extraites de ce processus

d'extension de la clé K par la fonction F. Plus précisément, on sait que la clé K peut être un mot de 128 bits, 192 bits ou 256 bits. Le message d'entrée ME est un mot de 128 bits. Toutes les combinaisons sont possibles et l'homme du métier choisit la combinaison qui représente le meilleur compromis, compte tenu du contexte, entre la rapidité d'exécution et le niveau de sécurité requis. Actuellement cependant, la plupart des algorithmes AES effectivement mis en œuvre font appel à une clé K de 128 bits. Les sous-clés K_0 ... K_n doivent être au format du message d'entrée. C'est pourquoi, chaque sous-clé est créée à partir d'un ou deux résultats successifs élaborés au cours du processus d'extension de clé par la fonction F. Dans l'exemple décrit, la clé K est codée sur 192 bits. Par conséquent, la sous-clé K_0 est extraite des deux premiers tiers de la clé K, la sous-clé K_1 est extraite de l'autre tiers de la clé K et du premiers tiers du résultat intermédiaire R_1 de la première transformation de cette clé par la fonction F, la sous-clé K_2 est extraite des deux derniers tiers du résultat intermédiaire R_1, et ainsi de suite jusqu'à l'élaboration de la dernière sous-clé K_n.

Du côté du traitement du message d'entrée, les opérations sont les suivantes. Ledit message d'entrée ME est combiné à la sous-clé K_0 par une fonction ou exclusif 16. Après quoi, le résultat est soumis à un groupe d'opérations (appelé ici ROUND 1) avec intervention de la sous-clé K_1. Puis, le résultat est soumis à nouveau à un groupe d'opérations dit ROUND 2 avec intervention de la sous-clé K_2, jusqu'à $ROUND_{n-1}$, dit dernier ROUND, avec intervention de la sous-clé K_{n-1}. Tous les "ROUNDS", de 1 à n-1, sont composés de quatre transformations. Un $ROUND_n$, dit ROUND final avec intervention de la sous-clé K_n comporte seulement trois transformations. Le résultat de ce round final est un message chiffré MC qui est renvoyé vers l'extérieur.

A la base de l'invention, on a mis en évidence que, si on est capable de provoquer des perturbations comme indiqué à des moments précis du déroulement de l'algorithme AES décrit ci-dessus, on peut retrouver tous les octets d'une sous-clé et plus particulièrement selon l'exemple, de la dernière sous-clé K_n de la façon suivante :

- si on provoque la perturbation au moment de l'application de la dernière fonction F, on arrive à retrouver des informations sur l'avant-dernière extension

de la clé par la fonction F, à savoir les quatre derniers octets de l'avant-dernier résultat R_{m-1}.

- si on parvient aussi à produire une perturbation au moment de l'exécution de l'avant-dernière extension par la fonction F, on peut retrouver les quatre octets voisins de R_{m-1}.

- si on provoque une perturbation sur le début du dernier round ($ROUND_{n-1}$), on arrive à retrouver 8 octets de la dernière extension de clé par la fonction F, c'est-à-dire R_m. Ces octets appartiennent à la sous-clé K_n.

- en traitant les résultats précédents, on arrive encore à retrouver six octets de plus répartis dans la dernière extension de clé R_m par la fonction F. Ces octets appartiennent aussi à la sous-clé K_n.

Pour retrouver les deux derniers octets de la sous-clé K_n, il est envisageable d'étudier toutes les possibilités jusqu'à retrouver ces deux derniers octets. Par conséquent, si la clé K avait été codée sur 128 bits, elle aurait pu être retrouvée à coup sûr par la seule mise en œuvre de l'attaque décrite ci-dessus. On rappelle que dans la majorité des algorithmes AES mis en œuvre actuellement, la clé K est effectivement codée sur 128 bits et il n'y a pas de différence entre les résultats intermédiaires R_1, R_2 ... R_m et les sous-clés K_1, K_2 ... K_n (dans ce cas, n = m) puisque chaque sous-clé est constituée de la totalité d'un résultat intermédiaire R_i correspondant. Dans l'exemple décrit cependant, la clé K a été codée sur 192 bits et l'attaque qui a été décrite dans ses grandes lignes ci-dessus ne permet pas de retrouver la clé puisque le résultat R_m n'est pas entièrement connu. On ne peut donc pas "remonter" jusqu'à la clé K à partir de ce résultat incomplètement connu. Cependant, on a affaibli considérablement la sécurité puisqu'on dispose d'informations partielles sur la clé, ce qui rend plus efficaces d'autres attaques (par exemple du type DPA) connues en soi.

Quoi qu'il en soit, la parade à ce type d'attaque consiste à mémoriser un résultat intermédiaire R_i, par exemple R_m, ou une sous-clé, par exemple ici la dernière sous-clé K_n, à refaire au moins une partie des étapes d'élaboration de la succession desdites sous-clés, c'est-à-dire essentiellement le processus d'extension de clé par la fonction F, jusqu'au recalcul d'un résultat correspondant à celui qui a été mémorisé. A partir de ce moment, on dispose de deux valeurs (de résultat intermédiaire ou de sous-clé) qui doivent être identiques si l'entité

électronique n'a été soumise à aucune attaque du type DFA. Il suffit de comparer la valeur du résultat ou sous-clé mémorisé à la valeur du résultat ou sous-clé recalculé correspondant et interdire la diffusion du message crypté MC issu du ROUND final si ces deux valeurs sont différentes. C'est ce qu'illustre la figure 3 où l'algorithme AES est complété (selon un mode de réalisation) en refaisant la totalité des étapes d'élaboration de la succession desdites sous-clés et plus particulièrement du processus d'extension de la clé K. Selon cet exemple, l'algorithme AES décrit en référence à la figure 2 est exécuté une première fois, le résultat est un message crypté MC. La dernière sous-clé K_n est mémorisée. Ensuite, on refait tout le processus d'extension de clé par la fonction F à partir de la clé K secrète de l'entité. Ceci aboutit à déterminer une nouvelle valeur de K_n. La valeur précédemment mémorisée et la nouvelle valeur sont comparées (test d'égalité). Si les deux valeurs sont égales, on autorise la sortie du message MC. Si les deux valeurs ne coïncident pas, la valeur MC n'est pas retransmise à l'extérieur et on peut émettre un message d'erreur.

Dans l'exemple qui vient d'être décrit, on refait la totalité du processus d'extension de clé jusqu'à obtenir le nouveau calcul de la dernière sous-clé K_n. Comme on l'a vu plus haut, on peut mémoriser un résultat intermédiaire R_i ou sous-clé, quelconque et refaire au moins une partie des étapes d'élaboration de la succession des sous-clés jusqu'au recalcul d'un résultat intermédiaire ou sous-clé correspondant à celui qui a été mémorisé. D'une façon générale, on a avantage, si on ne refait pas la totalité du cycle d'extension de clé par la fonction F, à refaire au moins une partie finale des étapes d'élaboration de la succession desdites sous-clés, c'est-à-dire plus particulièrement une partie finale du processus d'extension de clé par la fonction F, jusqu'à obtenir un second calcul du dernier résultat intermédiaire R_m ou de la dernière sous-clé.

Si on ne refait pas l'intégralité du processus itératif d'extension de clé (à partir de la clé K), il faut évidemment mémoriser le résultat intermédiaire (ou la sous-clé) d'où on repart.

L'invention n'est pas limitée à la sécurisation de l'algorithme AES. A titre d'exemple, l'algorithme DES, également connu, est décrit à la figure 4. Brièvement, dans cet algorithme, le processus d'extension de la clé K est le suivant. La clé K (64 bits) est soumise à une permutation P1 sur les bits et

réduite à 56 bits. Le résultat est un mot 20 partagé en deux parties de 28 bits. Chacune d'elles est soumise à une permutation R (rotation circulaire sur les bits) de 1 ou 2 bits selon les cas. Les deux résultats sont rassemblés pour former un nouveau mot 21 de 56 bits soumis à une nouvelle permutation P2 et concaténé à 48 bits pour donner une sous-clé K_1. Par ailleurs, le mot 21 de 56 bits est traité de façon à subir deux rotations circulaires R pour aboutir à un nouveau mot 22, à nouveau soumis à la permutation P2 pour engendrer une sous-clé K2 et ainsi de suite jusqu'à K16. Par ailleurs, le message d'entrée ME de 64 bits subit les transformations suivantes. Il est d'abord soumis à une permutation P3 sur les bits et le résultat est soumis à des fonctions constituant le ROUND 1 faisant intervenir la sous-clé K1. On met ensuite en œuvre d'autres rounds successifs faisant intervenir d'autres sous-clés correspondantes (jusqu'à la sous-clé K16) et le résultat du dernier round est soumis à une permutation inverse $P3^{-}$. Le résultat de cette permutation inverse est le message chiffré MC destiné à être renvoyé.

On conçoit que la structure générale de l'algorithme DES qui vient d'être rappelée ci-dessus se prête bien à la mise en œuvre de l'invention. Il suffit par exemple de mémoriser la sous-clé K16 et de refaire tout ou partie du processus de diversification de la clé K composé de la permutation P1 et des rotations R. Le test peut même être réalisé sur la valeur du dernier résultat intermédiaire (mot 36) avant la dernière permutation P2. Dans ce cas, c'est ce dernier résultat qui est mémorisé et non pas la sous-clé K16.

Bien entendu, l'invention concerne aussi toute entité électronique, notamment toute carte à microcircuit, comportant des moyens de mise en œuvre du procédé décrit ci-dessus.

REVENDICATIONS

1. Procédé de sécurisation d'une entité électronique à accès crypté, laquelle comprend des moyens d'exécution d'un algorithme cryptographique consistant à appliquer à un message d'entrée une succession de groupes d'opérations dits "rounds" faisant intervenir une série de sous-clés (K_0 ... K_n) respectives, successivement élaborées par un processus itératif mis en œuvre à partir d'une clé initiale (K), caractérisé en ce qu'il consiste à mémoriser un résultat d'une étape intermédiaire (R_m, K_n) dudit processus itératif, à refaire au moins une partie des étapes dudit processus itératif jusqu'au recalcul d'un résultat correspondant à celui qui a été mémorisé, à comparer la valeur dudit résultat mémorisé à la valeur du résultat recalculé correspondant et à interdire la diffusion d'un message crypté (MC) résultant de la mise en œuvre dudit algorithme si ces deux valeurs sont différentes.

2. Procédé selon la revendication 1, caractérisé en ce qu'il consiste à mémoriser la valeur d'une sous-clé (K_n) et à refaire au moins une partie des étapes dudit processus itératif jusqu'au recalcul d'une sous-clé correspondant à ladite sous-clé mémorisée.

3. Procédé selon la revendication 1, caractérisé en ce qu'il consiste à mémoriser la valeur d'un résultat intermédiaire (R_m) dudit processus itératif et à refaire au moins une partie dudit processus itératif jusqu'au recalcul d'un résultat intermédiaire correspondant à celui qui a été mémorisé.

4. Procédé selon la revendication 2, caractérisé en ce qu'il consiste à mémoriser la valeur de la dernière sous-clé (K_n) et à refaire au moins une partie finale des étapes d'élaboration de la succession desdites sous-clés jusqu'à obtenir un second calcul de ladite dernière sous-clé.

5. Procédé selon la revendication 4, caractérisé en ce qu'il consiste à refaire la totalité des étapes d'élaboration de la succession desdites sous-clés.

6. Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il s'applique à un algorithme dit AES, connu en soi.

7. Procédé selon l'une des revendications 1 à 6, caractérisé en ce qu'il s'applique à un algorithme dit DES, connu en soi.

8. Entité électronique autonome caractérisée en ce qu'elle comporte des moyens de mise en œuvre (13) du procédé selon l'une des revendications précédentes.

9. Entité électronique selon la revendication 8, caractérisée en ce qu'elle est agencée sous forme de carte à microcircuit.

FIG.1

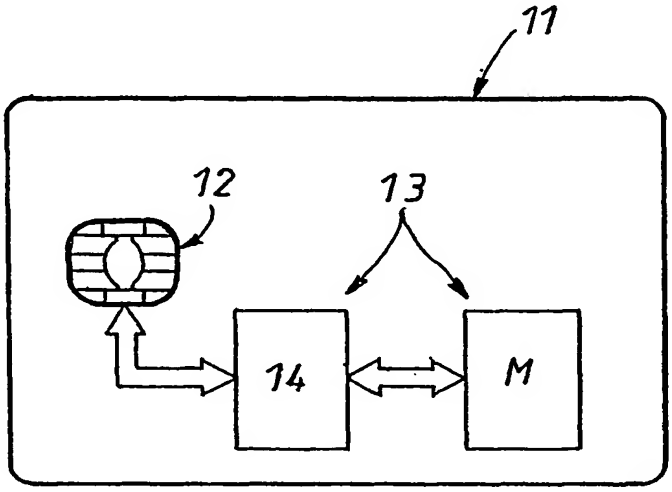

11
12
13
14
M

FIG.2

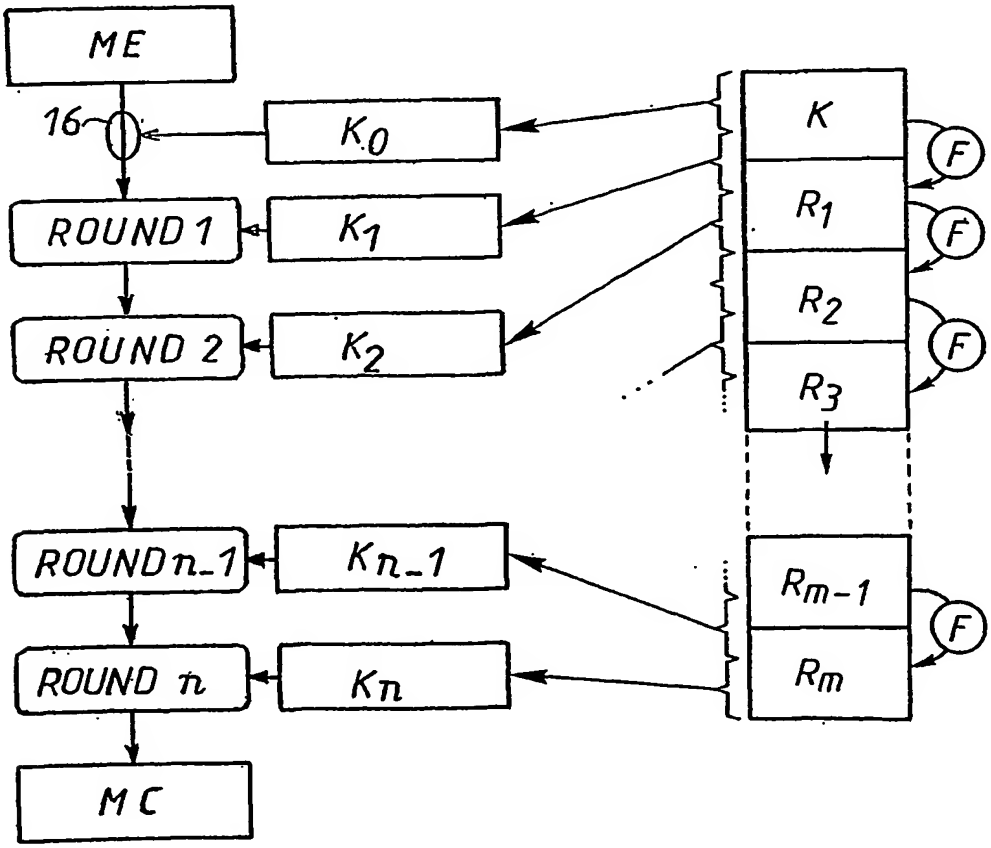

ME
16
K0
ROUND 1
K1
ROUND 2
K2
ROUND n-1
Kn-1
ROUND n
Kn
MC
K
R1
R2
R3
Rm-1
Rm
F

FIG.3

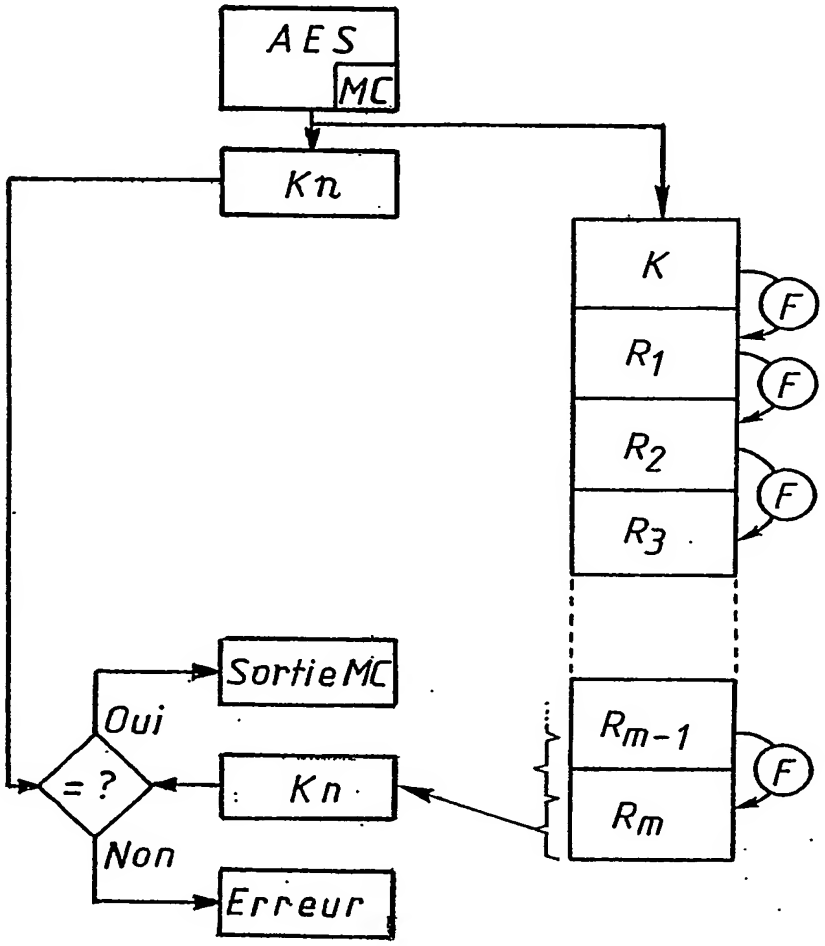
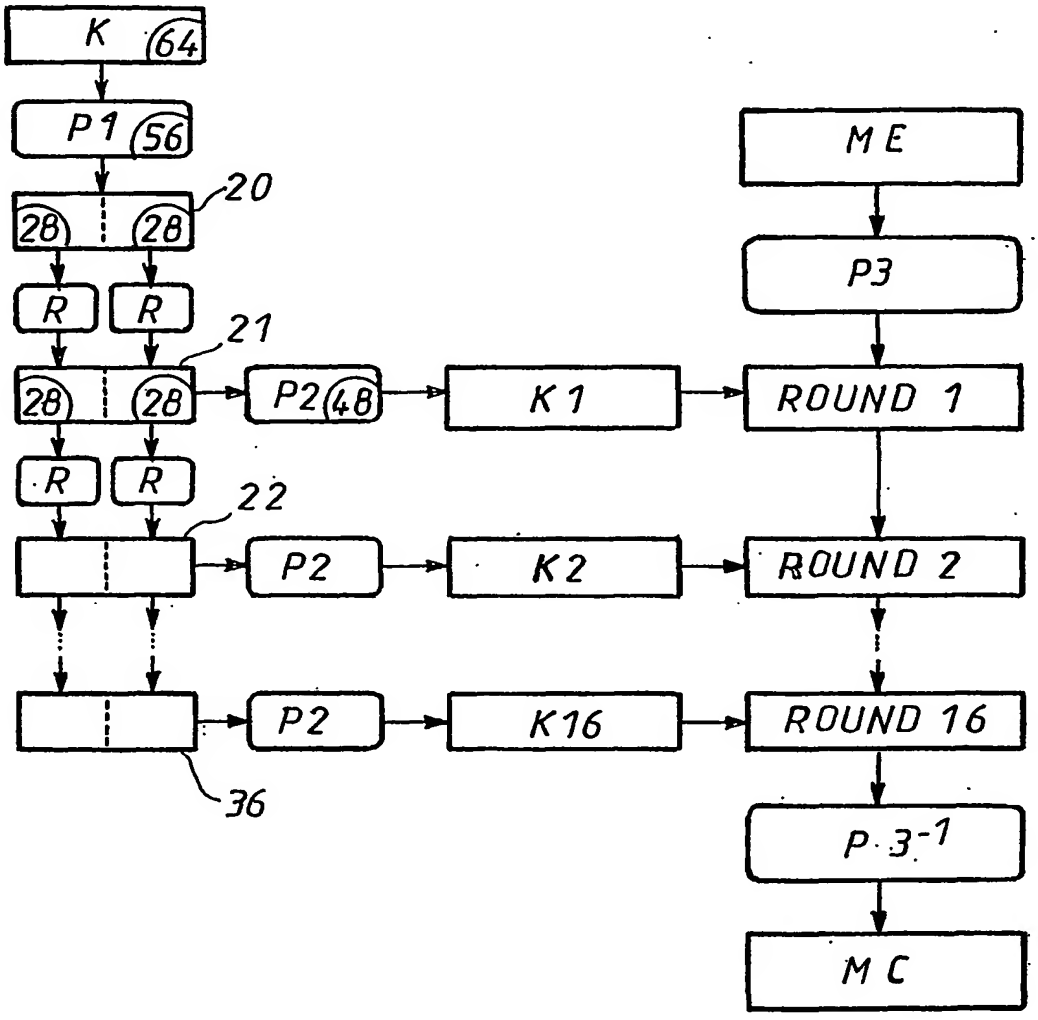


FIG. 4


K
64
P1
56
20
28
28
R
R
21
28
28
P2
48
K1
ROUND 1
R
R
22
P2
K2
ROUND 2
P2
K16
ROUND 16
36
ME
P3
P-3-1
MC

INTERNATIONAL SEARCH REPORT

Interna[redacted]al Application No
PC[redacted] 03/01032

A. CLASSIFICATION OF SUBJECT MA[redacted]
IPC 7 H04L9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
WPI Data, INSPEC, PAJ, EPO-Internal, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98 52319 A (YEDA RES & DEV ;FLEIT LOIS (US)) 19 November 1998 (1998-11-19) page 2, line 10 - line 20 page 9, line 3 - line 9	1,7
P,X	WO 03 024017 A (LIARDET PIERRE-YVAN ;SAGEM (FR); CHABANNE HERVE (FR); ST MICROELEC) 20 March 2003 (2003-03-20) page 8, line 14 -page 9, last line	1,3,7,8
A	US 6 108 419 A (BARKER BOBBY GLEN ET AL) 22 August 2000 (2000-08-22) abstract column 1, line 21 - line 28 column 3, line 3 - line 20	1

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
1 September 2003	10/09/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Intern[redacted]al Application No
PC[redacted]R 03/01032

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 9852319	A	19-11-1998	US	5991415 A	23-11-1999
			AU	7568598 A	08-12-1998
			EP	0986873 A1	22-03-2000
			WO	9852319 A1	19-11-1998
WO 03024017	A	20-03-2003	FR	2829331 A1	07-03-2003
			WO	03024017 A2	20-03-2003
US 6108419	A	22-08-2000	NONE		

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 03/01032

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/06

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
WPI Data, INSPEC, PAJ, EPO-Internal, IBM-TDB

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	WO 98 52319 A (YEDA RES & DEV ;FLEIT LOIS (US)) 19 novembre 1998 (1998-11-19) page 2, ligne 10 - ligne 20 page 9, ligne 3 - ligne 9	1,7
P,X	WO 03 024017 A (LIARDET PIERRE-YVAN ;SAGEM (FR); CHABANNE HERVE (FR); ST MICROELEC) 20 mars 2003 (2003-03-20) page 8, ligne 14 -page 9, dernière ligne	1,3,7,8
A	US 6 108 419 A (BARKER BOBBY GLEN ET AL) 22 août 2000 (2000-08-22) abrégé colonne 1, ligne 21 - ligne 28 colonne 3, ligne 3 - ligne 20	1

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
1 septembre 2003	10/09/2003

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Holper, G

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 03/01032

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 9852319	A	19-11-1998	US	5991415 A	23-11-1999
			AU	7568598 A	08-12-1998
			EP	0986873 A1	22-03-2000
			WO	9852319 A1	19-11-1998
WO 03024017	A	20-03-2003	FR	2829331 A1	07-03-2003
			WO	03024017 A2	20-03-2003
US 6108419	A	22-08-2000	AUCUN		